CHAPTER 9

ACCESS TO CLASSIFIED INFORMATION

9-1 BASIC POLICY

1. Access to classified information may be granted only if allowing access will promote the furtherance of the DON mission while preserving the interests of national security.

2. Access to classified information will be limited to the minimum number of individuals necessary to accomplish the mission and will be based on need to know. Additionally, the level of access authorized will be limited to the minimum level required to perform assigned duties. No one has a right to have access to classified information solely because of rank, position, or security clearance.

3. A Classified Information Nondisclosure Agreement (SF 312) must be executed by all persons prior to gaining initial access to classified information.

4. Commanding officers will ensure that personnel under their jurisdiction are briefed in accordance with paragraph 4-5 before granting access to classified information.

5. Under U.S. Navy regulations, the responsibility of the commanding officer for his or her command is absolute. Thus commanding officers have ultimate authority over who may have access to classified information under their control.

6. The Director, Naval Intelligence (DNI) is the Department of the Navy's Senior Official of the Intelligence Community (SOIC) with authority over all DON Sensitive Compartmented Information (SCI) access eligibility matters (paragraph 9-3 applies).

9-2 GRANTING ACCESS TO CLASSIFIED INFORMATION

1. Commanding officers may grant access to classified information to any individual who has an official need to know, an established security clearance, and about whom there is no known unadjudicated disqualifying information.

2. The determination to grant access to classified information is subject to the following restrictions:

a. DoD contractor employees holding only contractor-issued (company) Confidential clearances will not be granted access to Restricted Data, cryptographic information, SCI, or NATO information. (Other restrictions on DoD contractors for access to foreign intelligence information are described in SECNAVINST 5510.31B, Policy and Procedures for Control of Foreign Disclosure in the Department of the Navy, Dec 92).

b. For individuals who have not been determined to be eligible for security clearance, access authorization may be allowed in certian specific circumstances as discussed in this chapter. These unique access authorizations are specifically limited and are not reciprocally acceptable determinations.

c. The degree of access by representatives of foreign governments, including Personnel Exchange Program (PEP) personnel, will be scrupulously limited to that allowed by the Foreign Disclosure Authorization issued by the Navy International Programs Office (Navy IPO) on a case-by-case basis.

d. SCI access program management is governed by reference (c). Paragraph 9-3 synopsizes some of the procedures.

3. Granting access is a command responsibility. Access is formally terminated when it is no longer required in the performance of duties and/or when the individual's security clearance is denied or revoked.

4. Limiting access is the responsibility of each individual possessing classified information. Before allowing others access to classified information, individuals possessing classified information must determine that allowing access is justified based on the others' security clearance eligibility and need to know.

9-3 SENSITIVE COMPARTMENTED INFORMATION (SCI) ACCESS

1. The Navy Department Supplement to DoD Directive S5105.21. M-1, 18 Mar 97, reference (c), contains the policies and procedures for access to and dissemination of SCI.

2. The Director, DON CAF is delegated responsibility for granting, denying, revoking and verifying SCI access eligibility for DON personnel. In addition, the Director, DON CAF is also delegated the authority to adjudicate DON contractor personnel requiring SCI access eligibility under the NISP and reference (c).

3. The following procedures apply to initial requests for the DON CAF SCI access eligibility determinations:

a. A valid requirement or certification of need to know in accordance with reference (c) must be established prior to requesting the DON CAF adjudication for SCI access eligibility.

b. If it is determined that SCI access is required and a valid (e.g. conducted within the past 5 years) Single Scope Background Investigation (SSBI) does not exist, an SSBI request (or SSBI-PR if an outdated SSBI exists) will be sent to the Defense Security Service as directed by chapter 6.

c. If SCI access is required and a valid SSBI exists, the commanding officer will request an SCI access eligibility determination from the DON CAF using the OPNAV 5510/413. The collateral Top Secret security clearance required will be requested in conjunction with the SCI access eligibility request. The OPNAV 5510/413 must accurately reflect the citizenship of immediate family members because reference (c) imposes additional procedural requirements for individuals with foreign national immediate family members.

d. Upon favorable adjudication of the completed SSBI, the DON CAF will forward a final clearance/SCI access eligibility certification letter or message to the requesting command. Upon receipt of the DON CAF certification, the command will ensure the special security officer (SSO) receives a copy of the message or letter to indoctrinate the individual as directed by reference (c) and the security manager will maintain a command record of the clearance and access granted.

4. Requests for exceptions to DCID 1/14 for SCI access eligibility will be prepared as directed by reference (c) and forwarded to the DON CAF using the OPNAV 5510/413.

5. Commanding officers are responsible for establishing and administering a program for continuous evaluation of all personnel with security clearance and/or SCI access eligibility. Key to an active continuous evaluation program is security education. Continuous evaluation requirements are outlined in chapter 10 and in reference (c).

a. Information that could potentially affect an individual's eligibility for SCI access must be reported to the DON CAF with SSO Navy or COMNAVSECGRU as an information addressee in accordance with the procedures outlined in reference (c). The DON CAF will either reaffirm the SCI access eligibility or will

use the unfavorable determinations process outlined in chapter 7. Commanding officers may suspend, or debrief for cause from SCI access in accordance with reference (c). However, the decision to deny or revoke SCI access eligibility resides solely with the DON CAF. Additionally, the authority to review final appeals of unfavorable SCI access eligibility determinations is delegated to the Personnel Security Appeals Board (PSAB). The decision of the PSAB regarding SCI access is final.

b. A Periodic Reinvestigation (PR) is required every 5 years for individuals with SCI access. ALL PR requests will be forwarded to DSS, with the results returned to the DON CAF for adjudication. Chapter 6 describes the PR request process.

6. When an individual who is indoctrinated for SCI access is transferred-in-status to a new command, the gaining command SSO will forward an OPNAV 5510/413 to the DON CAF for revalidation of the SCI access eligibility. The losing command SSO will forward an SSO555 TIS message to the gaining command. Upon receipt of the SSO555 TIS message, the individual may be granted SCI access. Absent potentially disqualifying information, the DON CAF will send an SCI eligibility certification to the gaining command. If the certification is not received by the gaining command within 90 days of the individual's arrival, commands are required to send a copy of the originally submitted OPNAV 5510/413 boldly marked "TRACER." An OPNAV 5510/413 is not submitted on individuals in intelligence MOS/rating/designators (161X/163X, 644X, 654X, 744X, 754X, IS, CT, 26XX).

7. The commanding officer may debrief an individual from SCI access for administrative reasons as provided in reference (c).

8. The DON CAF will record the SCI access eligibility determination in the NJACS which feeds the DON personnel data displayed in the ODCR, EDVR, MCTFS, and DCPDS. SCI access eligibility is also reflected in the DCII.

9-4 CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT (SF 312)

1. A Classified Information Nondisclosure Agreement (NdA), Standard Form (SF) 312 must be executed by all personnel as a condition of access to classified information. An example of the SF 312 is provided at exhibit 9A.

2. The current SF 312, (Rev. 1-91), supersedes the SF 189, Classified Information Nondisclosure Agreement, the SF 189-A, Classified Information Nondisclosure Agreement (Industrial/

Commercial/Non-Government) and the SF 312 (Rev. 9-88), Classified Information Nondisclosure Agreement. Previously executed SF 312's remain valid and will be understood to be amended to reflect the language of the most current SF 312 (Rev. 1-91). All NdAs previously executed will be interpreted and enforced in a manner fully consistent with the interpretation and enforcement of the SF 312 (Rev. 1-91).

3. DON military and civilian employees who have not previously signed an SF 312 must sign a current SF 312 before being given initial access to classified information.

4. When the DON CAF initially grants a security clearance, commands will be directed to ensure an SF 312 is appropriately executed as a condition of allowing access to classified information. Personnel who have signed other nondisclosure agreements for specific access (such as Form 1847-1, Sensitive Compartmented Information (SCI) Non-Disclosure Agreement), must also execute the SF 312.

5. If an individual refuses to sign an SF 312, the command will deny the individual access to classified information and report the refusal to the DON CAF.

6. Commanding officers will ensure personnel are provided an explanation of the purpose of the SF 312 and have the opportunity to read the Sections of Titles 18 and 50 of the United States Code and other references identified on the SF 312.

7. The execution of the SF 312 must be witnessed and the witnessing official must sign and date the NdA at the time it is executed. The witnessing official can be any member of the command. The SF 312 must be accepted on behalf of the United States. The accepting official can be the commanding officer, the executive officer, the security manager, or an individual designated in writing by the commanding officer to accept the SF 312 on behalf of the U.S. Government.

8. Executed SF 312's will be maintained for 70 years from date of signature.

9. The completed forms will be forwarded to the following addresses for retention:

Navy military members:
Commander, Naval Personnel Command
Pers 313C1
5720 Integrity Drive
Millington, TN 38055-8310

Marine Corps military members:
Commandant of the Marine Corps
Headquarters US Marine Corps (MMSB-22)
MCCDC
2008 Elliot Road
Suite 114
Quantico VA 22134-5030

All DON civilian personnel:
To their Official Personnel Folder (OPF)

10. A SF 312 need only be executed once by an individual when initially granted access. Administrative withdrawal of clearance, after execution of an SF-312, and subsequent granting of clearance and access will neither require validation of the previous execution nor reexecution of another SF-312.

11. For reservists who will have initial access to classified information, the reserve unit security manager will ensure execution of the SF 312 prior to forwarding the member to the duty assignment in which access to classified information will be required.

12. Contractor, licensee, and grantee employees or other non-government personnel will sign the SF 312 before being authorized access to classified information.

9-5 RECORDING ACCESS

1. The DON CAF maintains the official record of security clearances granted and initial access determinations in the Navy Joint Adjudication and Clearance System (NJACS).

2. Command security managers are responsible for maintaining a record of all access granted to include temporary accesses, special accesses or other program accesses formally granted (e.g. SIOP-ESI, NATO Secret, CNWDI, COSMIC, SCI, and PRP). Requirements for SSO's maintaining records of SCI access determinations are provided in reference (c).

3. Each command may use a method of record maintenance suited to the command's capabilities, such as a computerized database, a

log book, or a form OPNAV 5520/20, and must maintain the record for 2 years after access terminates.

4. The command access record must include the following data elements: Name, SSN, citizenship verification, date and level of access authorized, the basis for the access determination and the name and title, rank or grade of the individual authorizing the access. Interim security clearance and certain temporary accesses are recorded on the OPNAV 5510/413.

5. The command security manager is responsible for notifying an individual's supervisor when access has been granted with specific instructions regarding restrictions or limitations.

9-6 ONE-TIME ACCESS

1. An urgent operational or contractual emergency may arise for cleared personnel to have one-time or short duration access to classified information at a level higher than that for which they are eligible. Processing the individual to upgrade the security clearance would not be practical in these situations, therefore an individual may be granted access at one security classification level above that for which eligible, subject to the following terms and conditions:

a. One-time access may only be granted by a flag or general officer, a general courts-martial convening authority or equivalent Senior Executive Service member, after coordination with command security officials.

b. The individual granted one-time access must be a U.S. citizen, have a current DoD security clearance and have been continuously employed by DoD or a cleared DoD contractor for the preceding 24-month period. One-time access is not authorized for part-time or temporary employees.

c. Review of locally available records has been conducted as provided in paragraph 6-12.1b and revealed no disqualifying information.

d. Whenever possible, access will be limited to a single instance or, at most, a few occasions. If repeated access is required, the proper personnel security investigation will be initiated.

e. Approval for access will automatically expire no later than 30 calendar days from the date access commenced. If the need for access is expected to continue for a period in excess of

30 days, written approval is required from CNO (N09N2). If the need for access is expected to extend beyond 90 days, the command must initiate a request for the appropriate security clearance. Access will not be extended, in any case, beyond 90 days from the date access commenced unless a supporting personnel security investigation is requested.

f. Access at the higher level will only be allowed under the supervision of a properly cleared individual. The supervisor will be responsible for recording (paragraph 9-5.3 applies) the higher level information actually revealed with the dates access was afforded and for retrieving the accessed material daily.

g. Access will be limited to information under the control of the official who authorized the one time access. Access at the next higher level will not be authorized for COMSEC, SCI, NATO or foreign government information.

2. This provision will be used sparingly and repeated use of one time access within any 12 month period on behalf of the same individual is prohibited.

3. A record must be maintained for each individual authorized one time access. The record will include the following information:

a. The name and social security number of the individual;

b. The level of access authorized;

c. Justification for the access, to include an explanation of the compelling reason to grant the higher level access and, specifically, how the DON mission would be furthered;

d. An unclassified description of the specific information to which access was afforded and the duration of the access, to include the dates access was afforded;

e. A listing of the locally available records reviewed and a statement that no significant adverse information concerning the individual is known to exist;

f. The approving authority's signature; and

g. Copies of any pertinent briefings/debriefings given to the individual.

9-7 TEMPORARY ACCESS

1. Temporary access may be granted to DON personnel who have been otherwise determined to be eligible for a security clearance by the DON CAF but do not currently require a security clearance/access to perform assigned duties. Before authorizing temporary access, the commanding officer must determine that it is to the DON's benefit to allow disclosure to an individual who does not require access in the usual performance of duties. Situations in which temporary access may be justified include attendance at a classified meeting or training session, participation in advancement examinations, or annual reserve active duty for training or scheduled inactive duty training.

2. If temporary access is justified, the commanding officer may, after favorable review of locally available records in accordance with paragraph 6-12.1b, allow access or certify to another command the individual's security clearance eligibility as a basis to allow access to classified information.

3. This provision must be monitored very carefully and exercised only when access is needed for a limited time. Authority to allow temporary access does not include access to SCI or NATO information. Procedures for temporary access to SCI are provided by reference (c).

9-8 TEMPORARY ACCESS PENDING RECEIPT OF CLEARANCE CERTIFICATION

1. Temporary access may be granted when a member reports to a command and there are clear indications that a security clearance which could support the access required was previously granted but the DCII is unavailable for local validation and there is no DON CAF security clearance certification in the individual service record or official personnel folder. (This does not apply to SCI access.)

2. Commands will submit an OPNAV 5510/413 to the DON CAF indicating the level of security clearance required (item 20) and will maintain a tickler copy for tracer purposes. If the command does not receive a current DON CAF security clearance certification within 90 days, commands are required to send a copy of the originally submitted OPNAV 5510/413 boldly marked "TRACER." If after 180 days the command does not receive the required certification, temporary access must be terminated. Commands will initiate direct dialog with the DON CAF to determine if a request for security clearance is required.

3. Commands with DCII access may use DCII data in lieu of requesting the DON CAF clearance certification. Instructions for establishing command DCII access can be found in appendix E.

9-9 ACCESS BY RETIRED PERSONNEL

1. Retired personnel, including those on the temporary disability retirement lists, are not entitled to have access to classified information merely by virtue of their present or former status. When a commanding officer decides to grant a retiree access to classified information in the furtherance of the DON mission, a request for access authorization may be submitted to CNO (N09N2) using the guidance contained in paragraph 9-14.

2. As an exception to the above, an active duty flag/general officer may waive the investigative requirement and grant a retired flag/general officer temporary access to classified information when he/she determines that there are compelling reasons in furtherance of a DON program or mission to grant such access. The period of access will not exceed 180 days.

a. Access may only be granted to information classified at a level commensurate with the security clearance held by the retired flag/general officer at the time of his/her retirement. Granting access to SCI is prohibited.

b. Access will be granted only under the condition that the retiree not remove classified materials from the confines of a government installation or other area approved for storage of classified information.

c. The flag/general officer granting the access will inform CNO (N09N2) of this event by a written report within 5 days. The report must identify the retired flag/general officer involved, the classification of the information to which access was authorized, the DON program or mission which is served by granting access, and the period of time for which access is authorized.

d. If continued access beyond the 180 day limit is necessary, the report to CNO (N09N2) must be accompanied by requests for the appropriate personnel security investigation and clearance.

9-10 ACCESS BY RESERVE PERSONNEL

1. Reserve personnel in an "**active status**" may be granted access as necessary, provided they hold the appropriate security clearance eligibility. For Active Duty for Training (less than 30 days) and inactive duty training (drills) procedures described in paragraph 9-7 may apply.

2. Reserve personnel may also be given access to Communications Security (COMSEC) information necessary to maintain proficiency in their specialty. Details are provided in CMS-1A, Cryptographic Security Policy and Procedures Manual (U), 25 Feb 98, (NOTAL).

9-11 ACCESS BY INVESTIGATIVE AND LAW ENFORCEMENT AGENTS

1. Investigative agents of other departments or agencies may obtain access to classified information only through coordination with the Naval Criminal Investigative Service (NCIS).

2. The NCIS will be responsible for verifying the need to know of the other agency requiring the access.

9-12 ACCESS AUTHORIZATION FOR ATTORNEYS

1. Requests for access authorization for attorneys representing DON personnel will be submitted to CNO (N09N2) via the Office of General Counsel (OGC) or Navy Judge Advocate General (NJAG). Requests will provide a brief summary of the facts of the case and a description of the specific classified information the defense will require to adequately represent his or her client.

2. OGC or NJAG will evaluate the request and certify that access to the specified classified information is necessary and will ensure the attorney requiring the access has completed the necessary investigative request forms. OGC or NJAG will then forward the certified access request, including the investigative request forms, to CNO (N09N2).

3. CNO (N09N2) will submit the request for investigation to DSS and will authorize access, as appropriate. Prior to access the attorney will be required to sign the Classified Information Nondisclosure Agreement (SF 312).

9-13 CONTRACTOR ACCESS

1. Commanding officers may grant access to classified information to contractor employees based on the contractors need to know and the contracting facilities certification of security clearance provided on the classified visit request. Paragraph 11-2 provides visit request details.

2. Commanding officers may, at any time, deny contractor employees access to areas and information under command control for cause. However, suspension or revocation of contractor security clearances can only be effected through DSS. Action taken by a command to deny a contractor access to the command areas and information will be reported to the DSS OCC with an information copy to the DSS Operating Location Office (OPLOC). If SCI access is an issue, a report will also be forwarded to the DON CAF.

3. Contractor-granted Confidential clearances in effect under previous policy are not valid for access to Restricted Data, Formerly Restricted Data, cryptographic or intelligence information, Naval Nuclear Propulsion Information, NATO information (except Restricted), SCI, and foreign government information.

9-14 ACCESS AUTHORIZATION FOR PERSONS OUTSIDE OF THE EXECUTIVE BRANCH OF THE GOVERNMENT

1. When an individual who is outside the Executive Branch of the Government has a special expertise that can be employed in furtherance of the DON mission, a commanding officer may request CNO (N09N2) to authorize the access, provided the individual is a U.S. citizen and the information being accessed is information for which the commanding officer is responsible.

2. A request for access will be submitted to CNO (N09N2) for access authorization. The request will include:

a. Full name, date and place of birth and social security number;

b. The justification of the need for the access;

c. The expertise the individual will bring to the program or project;

d. The classification level, nature and scope of the information to be accessed;

e. The period of time for which access is required (not to exceed 24 months); and

f. The appropriate personnel security investigative request package, completed in accordance with paragraph 6-14.

3. CNO (N09N2) will not accept a request from the individual desiring access. Requests for access must be sponsored by an active duty commanding officer who will assume responsibility for ensuring the individual is briefed on their responsibilities for protecting classified information, that a Classified Information Nondisclosure Agreement (SF 312) is executed and proper safeguards and limitations are employed.

4. Access will be granted only as specifically authorized by CNO (N09N2) and limited to the classified information identified in the request. The access authorization will be effective for the period of time necessary, but no longer than 2 years.

5. Physical custody of classified material will not be allowed.

6. The command will record the access authorized and maintain the record for 2 years after expiration of the access.

9-15 HISTORICAL RESEARCHERS

Individuals outside the Executive Branch of the Government engaged in private historical research projects may be granted access to classified information if steps are taken to ensure that classified information or material is not published or otherwise compromised.

a. Requests for access authorization for DON classified information will be processed by the Director of Naval History, Office of the Chief of Naval Operations (CNO (N09BH)) or the Director of Marine Corps History and Museums (CMC (Code HD)), Headquarters Marine Corps. Upon receipt of a request for access authorization, CNO (N09BH) or CMC (Code HD) will seek to declassify the requested records. If declassification cannot be accomplished, CNO (N09BH) or CMC (Code HD) will:

(1) Prepare a recommendation as to whether the access requested would promote the interests of national security in view of the intended use of the material;

(2) Obtain from the researcher completed investigative request forms appropriate for the level of access required and submit them with the recommendation requesting access

authorization to CNO (N09N2), who will advise whether access is authorized for the specific project;

(3) Have the researcher sign a Classified Information Nondisclosure Agreement (SF 312);

(4) Limit the researcher's access to specific categories of information over which the DON has classification jurisdiction or to information within the scope of the historical research if the researcher has obtained written consent from the DoD or non-DoD departments or agencies with classification jurisdiction over that information;

(5) Retain custody of the classified information at a DON installation or activity or authorize access to documents in the custody of the National Archives and Records Administration; and

(6) Obtain the researcher's written agreement to safeguard the information and to submit any notes and manuscript for review by the DON or other DoD or non-DoD department or agency with classification jurisdiction, to determine that they do not contain classified information.

b. Access authorizations are valid for not more than 2 years from the date of issuance. Extensions may be granted by CNO (N09N2), if recommended by CNO (N09BH) or CMC (Code HD).

9-16 LIMITED ACCESS AUTHORIZATION (LAA) FOR NON-U.S. CITIZENS

1. Although non-U.S. citizens are not eligible for security clearance, access to classified information may be justified for compelling reasons in furtherance of the DON mission, including special expertise. An LAA may be justified in those rare circumstances where a non-U.S. citizen possesses a unique or unusual skill or expertise that is urgently needed and for which a cleared or clearable U.S. citizen is not available. When justified, an LAA may be considered under the following conditions:

a. Access is limited to classified information relating to a specific program or project;

b. Appropriate foreign disclosure authority determines that access to classified information is not inconsistent with releasability to the individual's country of origin;

c. Physical custody of classified material will not be authorized;

d. LAAs will not be granted to personnel who perform routine administrative or other support duties;

e. Individuals granted LAAs will not be designated couriers or escorts for classified material unless they are accompanied by an appropriately cleared U.S. person;

f. Personnel granted LAA's will not be permitted uncontrolled access to areas where classified information is stored or discussed. Classified information will be maintained in a location that will be under the continuous control and supervision of an appropriately cleared U.S. citizen.

g. An SSBI is completed favorably; where full investigative coverage cannot be completed, a counterintelligence-scope polygraph examination will be required; and

h. A foreign national employee must agree to a counterintelligence-scope polygraph examination before being granted access. Failure to agree will terminate the processing of the LAA request.

2. When an LAA appears to be justified, a commanding officer may submit a request to CNO (N09N2) with the following information:

a. The identity of the individual for whom LAA is requested, including name, date and place of birth, current citizenship, social security number (if held),

b. Status as an immigrant alien or foreign national; if an immigrant alien, the date and port of entry and alien registration number;

c. Date and type of most recent personnel security investigation. If an SSBI has not been completed within the past 5 years, the completed personnel security investigative request package must be enclosed;

d. Level of access required;

e. The position requiring access and the nature and identity of the specific program material (delineated as precisely as possible) for which access is requested;

f. The compelling reasons for the request including an explanation of the special skills or special expertise the individual possesses and the rationale for not employing a cleared or clearable U.S. citizen;

g. An explanation as to how the command plans to control and limit the individual's access;

h. A statement that the candidate has agreed to undergo a counterintelligence scope polygraph examination when needed; and

i. The period of time for which access is required. (Will not exceed 5 years).

3. CNO (N09N2) will review the LAA request to determine if the justification provided meets the program requirements. If the justification is not adequate the LAA request will be promptly returned to the requester. If the justification is adequate, CNO (N09N2) will forward the SSBI request to DSS, however, the decision to authorize limited access can not be made until favorable adjudication of the completed SSBI.

4. CNO (N09N2) will coordinate foreign disclosure decisions with the Navy International Programs Office (Navy IPO), when required.

5. Individuals with LAAs will be placed under the general supervision of appropriately cleared persons. Supervisors will be made fully aware of the limits to access imposed and that physical custody of classified information by the individual is not authorized. A Classified Information Nondisclosure Agreement (SF 312) must be executed by the individual prior to granting access to classified information.

6. Individuals who have been granted a LAA will not be allowed to have access to any classified information other than that specifically authorized.

7. If an individual granted a LAA is transferred to another position, the LAA previously granted is rescinded. The individual will be debriefed in accordance with chapter 4. If the individual is transferring to other duties requiring a LAA, the command will request a new access authorization. If the individual's SSBI is less than 5 years old in these cases a new PSI is not required.

8. Periodic Reinvestigations (PR) are required every 5 years for individuals with LAA. Because LAA's are not authorized for more than 5 years, a new request for LAA must accompany a request for PR. CNO (N09N2) will review the justification and promptly notify the command to either continue the LAA until favorable completion of the PR by DSS or to discontinue access authorized based on lack of justification.

9. Non-U.S. citizens will not be authorized access to foreign intelligence information without approval of the originating agency, or to COMSEC keying materials, Top Secret, Naval Nuclear Propulsion Information (NNPI), TEMPEST, cryptographic or NATO information.

9-17 TERMINATING, WITHDRAWING OR ADJUSTING ACCESS

1. Access terminates when an individual transfers from a command. Commands will debrief individuals as outlined in paragraph 4-11, but execution of a Security Termination Statement is not required because affiliation continues and clearance requirements will normally remain.

2. Commanding officers will administratively withdraw an individual's access when a permanent change in official duties (i.e. rating/MOS changes) eliminates the requirement for security clearance and access and when the individual separates from the DON or otherwise terminates employment. The individual will be debriefed as outlined in paragraph 4-11 and will execute a Security Termination Statement which will be filed in the individual's service record or official personnel folder. Commands will forward an OPNAV 5510/413 to notify the DON CAF that the individual no longer requires clearance and access. The DON CAF will adjust the NJACS accordingly.

3. When the level of access required for an individual's official duties change, the command will adjust the authorized access accordingly, provided the new requirement does not exceed the level allowed by the security clearance. If the level of access required will exceed the level allowed by the DON CAF security clearance certification, the command will request the appropriate investigation and may consider interim clearance procedures as specified in paragraph 8-5.

9-18 SUSPENSION OF ACCESS FOR CAUSE

1. When questionable or unfavorable information becomes available concerning an individual who has been granted access, the commanding officer may suspend access. Suspension of access for cause may only be used as a temporary measure which must be resolved through either a favorable or unfavorable security determination by the DON CAF prior to the individual being transferred to a different command. The commanding officer will forward all pertinent information concerning the individual to the DON CAF for a final security clearance determination.

a. Suspension of access is required when a civilian employee with security clearance is incarcerated (to include Work Release Programs) as the result of a conviction for a criminal offense or is absent without leave for a period exceeding 30 days.

b. Suspension of access is required when a military member with a security clearance is discharged under Other Than Honorable conditions, is incarcerated (to include Work Release Programs) as the result of a conviction for a criminal offense or violations of the Uniform Code of Military Justice (UCMJ), is declared a deserter or is absent without leave for a period exceeding 30 days.

2. Whenever a determination is made to suspend access to classified information the following is required:

a. The individual concerned must be notified of the determination **in writing** by the commanding officer or designee, to include a brief statement of the reason(s) for the suspension action consistent with the interests of national security;

b. Commands and activities must report all suspensions to the DON CAF no later than 10 working days from the date of the suspension action using the OPNAV 5510/413 detailing the questionable or unfavorable information which caused the suspension action;

c. Take steps to ensure that the individual's clearance certification is removed from records, the individual's name is removed from all local access rosters and visit certifications, and all coworkers are notified of the suspension;

d. Ensure that the combination to classified storage containers to which the individual had access are changed unless sufficient controls exist to prevent access to the lock;

e. Place a copy of the OPNAV 5510/413 report to the DON CAF of the suspension of access in the individual's local service record or OPF, pending a final determination by the DON CAF;

f. Cancel or hold in abeyance any Permanent Change of Station (PCS) orders. Notify CHNAVPERS (Pers-831) for Navy military members or HQ USMC (INTC) for Marine military members under orders.

3. A determination to suspend SCI access for cause will include suspension of the security clearance.

9-19 ACCESS TO AND DISSEMINATION OF RESTRICTED DATA (RD) INCLUDING CRITICAL NUCLEAR WEAPON DESIGN INFORMATION (CNWDI)

1. Restricted Data (RD), as defined in the Atomic Energy Act of 1954 as amended is data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but does not include data declassified or removed from the RD category under Section 142 of the Act.

a. Access to RD within and between DON commands, National Aeronautics and Space Administration (NASA) and contractor activities will be governed by the same procedures and criteria as govern access to other classified information:

(1) Access is required in the performance of official duties.

(2) The individual has a valid security clearance commensurate with the level of access required for the information.

b. Requests for access to RD not under the control of DoD and/or NASA will be made in accordance with DoD 5210.2, Access to and Dissemination of Restricted Data, 12 Jan 78 (NOTAL).

(1) Requests by members of DON commands requiring access to RD at DOE facilities will be made utilizing the DOE Visit Request Form 5631.20, Request for Visit Approval or Access Approval and will be submitted via the appropriate DON certifying official identified by DoD 5210.2 to the Associate Deputy Assistant Secretary for Technical and Environment Support (DP-45), Department of Energy, Washington, DC 20585.

(2) Conflicts in guidance and inquiries relating to access and/or the protection of RD by DON personnel and commands should be referred to CNO (N09N2) for resolution.

c. The following procedures apply to DON commands and personnel who disseminate RD under their control:

(1) Within and between DoD commands, to include DoD contractors, dissemination of RD information will be governed by the same procedures and criteria as govern the dissemination of other classified information; verify the identity of the prospective recipient, verify the prospective recipient's

clearance and insure the prospective recipient has an official "need to know."

(2) Dissemination of RD and Formerly Restricted Data (FRD) outside DoD will be made in accordance with DoD 5210.2.

2. Critical Nuclear Weapon Design Information (CNWDI) is Top Secret Restricted Data or Secret Restricted Data that reveals the theory of operation or design of the components of a thermonuclear or implosion type fission bomb, warhead, demolition munitions, or test device. Specifically excluded is information concerning arming, fuzing, and firing systems; limited life components; and total contained quantities of fissionable, fusionable, and high explosive material by type. Among these excluded items are the components that DoD personnel set, maintain, operate, test or replace.

a. Access to and dissemination of CNWDI is of particular concern due to the extreme sensitivity of this type of information. Access must be limited to the absolute minimum number of persons needed to meet mission requirements. To meet this objective, the following special requirements and procedures for controlling CNWDI information have been established:

(1) Final TOP SECRET or SECRET Clearance (as appropriate)

(2) Except in rare instances only U.S. citizens will be granted access. When an immigrant alien possesses unique or very unusual talents and/or skills that are essential to the U.S. Government that are not possessed to a comparative degree by an available U.S. citizen, a request with justification to use such individual will be forwarded to CNO (N09N2) for approval.

(3) Requests by members of DON commands for access to CNWDI at DOE facilities will be made utilizing DOE Visit Request Form 5631.20 and must be submitted via an appropriate DON certifying official to the Associate Deputy Assistant Secretary for Technical and Environment Support (DP-45), Department of Energy, Washington, DC 20585. DoD 5210.2 contains a listing of DON officials authorized to certify access to CNWDI at DOE facilities. Recommendations for changes to the list of DON approved certifying officials will be submitted, with supporting justification to CNO (N09N2) for approval and inclusion in DoD 5210.2.

(4) Verification of "need to know". Certifying officials will not automatically approve requests for access to CNWDI, but will insist upon full justification and will reject any requests

that are not completely justified. Certifying officials have a special responsibility to insure that this "need to know" principle is strictly enforced.

(5) Personnel having a need for access to CNWDI will be briefed on its sensitivity. Briefings and access authorizations will be recorded in appropriate security records and maintained in a manner that facilitates verification. Similarly, personnel whose CNWDI access is terminated (reassignment, etc.) must be debriefed. Individual briefing/debriefing records will be maintained 2 years after access is terminated. Each DON command will establish their own procedures and format for briefing/debriefing.

b. For additional guidance refer to DoD 5210.2 or contact CNO (N09N2).

EXHIBIT 9A

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN _____ AND THE UNITED STATES

(Name of Individual - Printed or typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12356, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Sections 1.1 and 1.2(e) of Executive Order 12356, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of the information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or the termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, and *952, Title 18, United States Code, *the provisions of Section 783(b), Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of classified information not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of Section 793, Title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Ageement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

10. These restrictions are consistent with and do not supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 12356; Section 7211 of Title 5; United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, and 952 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

(Continue on reverse.)

NSN 7540-01-280-5499
Previous edition not usable.
312-102
STANDARD FORM 312 (REV. 1-91)
Prescribed by GSA/ISOO
32 CFR 2003, E.O. 12356

11. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this Agreement and its implementing regulation (32 CFR Section 2003.20) so that I may read them at this time, if I so choose.

SIGNATURE	DATE	SOCIAL SECURITY NUMBER (See Notice below)

ORGANIZATION (IF CONTRACTOR, LICENSEE, GRANTEE OR AGENT, PROVIDE: NAME, ADDRESS, AND, IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER) (Type or print)

WITNESS		ACCEPTANCE	
THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.		THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.	
SIGNATURE	DATE	SIGNATURE	DATE
NAME AND ADDRESS (Type or print)		NAME AND ADDRESS (Type or print)	

SECURITY DEBRIEFING ACKNOWLEDGEMENT

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.

SIGNATURE OF EMPLOYEE	DATE

NAME OF WITNESS (Type or print)	SIGNATURE OF WITNESS

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above or 2) determine that your access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations, or possibly result in the denial of your being granted access to classified information.

* NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT.

STANDARD FORM 312 BACK (REV. 1-91)